

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Pemakaian perangkat teknologi berbasis *wireless* pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi *wireless* memanfaatkan frekwensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh user maupun oleh operator yang memberikan layanan komunikasi.

Hal tersebut juga dilakukan di Balai Besar Penanaman dan Penelitian Tanaman Obat dan Obat Tradisional (B2P2TO2T) Tawangmangu, Karanganyar. Di balai tersebut memiliki aset informasi (*hardware, software, sistem, informasi dan manusia*) merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi). Untuk itu butuh pengelolaan keamanan informasi yang sistemik dan komprehensif.

Keamanan sistem informasi berbasis internet harus sangat diperhatikan, karena jaringan komputer internet yang sifatnya publik dan *global* pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam *internet*, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user *Internet* yang lain untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif.

Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan *wireless* terbentang di atas empat layer di mana keempat lapis (*layer*) tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media *wireless*. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi *wireless* tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas *MAC filtering*, pemasangan infrastruktur *captive portal*.

Berdasarkan uraian di atas, penulis tertarik untuk menganalisa cara serta mengamankan suatu sistem dan jaringan LAN dengan menggunakan NMAP dan

HPING3. Dimana akan membawa pengaruh positif terhadap keamanan jaringan LAN pada B2P2TO2T agar lebih efektif.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang yang telah diuraikan, untuk memudahkan proses penelitian ini, penulis merasa perlu adanya suatu rumusan yang tepat. Sehingga dapat memperjelas masalah yang akan diteliti. Adapun perumusan masalahnya adalah “Bagaimana sistem keamanan pada jaringan LAN dengan menggunakan NMAP dan HPING3 di B2P2TO2T, Karanganyar Tawangmangu?”

## **1.3 Batasan Masalah**

Penelitian ini akan membahas sistem keamanan pada jaringan LAN dengan menggunakan NMAP dan HPING3 di Balai Besar Penelitian dan Penanaman Tanaman Obat dan Obat Tradisional dengan menggunakan NMAP dan HPING3

*Software* yang digunakan untuk menganalisa keamanan jaringan LAN dalam penelitian ini adalah NMAP dan HPING3. Penulis akan menganalisa jaringan LAN pada Balai Besar Penelitian dan Penanaman Tanaman Obat dan Obat Tradisional, Tawangmangu, Karanganyar

## 1.4 Tujuan Penelitian

Tujuan penulisan dari proyek akhir ini adalah menganalisa performa keamanan jaringan internet dan mengetahui *vulnerability* dari suatu jaringan, dengan menggunakan NMAP dan HPING3 sehingga dengan mengetahui kelemahan yang terdapat pada jaringan maka langkah-langkah untuk mengatasi kelemahan ini dapat dilakukan.

Penganalisaan keamanan jaringan LAN ini, diharapkan keamanan dalam data-data di Balai Besar Penelitian dan Pengembangan Tanaman Obat dan Obat Tradisional, Tawangmangu, Karanganyar lebih terjaga keamanannya

## 1.5 Manfaat Penelitian

Setelah penelitian ini dilaksanakannya diharapkan dapat memberikan manfaat yaitu:

1. Penulis bisa menerapkan ilmu yang diperoleh semasa perkuliahan untuk menyelesaikan karya ilmiah berupa skripsi di Balai Besar Penelitian dan Pengembangan Tanaman Obat dan Obat Tradisional, Tawangmangu, Karanganyar.
2. Pada instansi tersebut dapat mengetahui kelemahan keamanan jaringan LAN mereka
3. Keamanan jaringan LAN dapat dimaksimalkan
4. Penulis dapat mengetahui metode-metode yang digunakan dalam keamanan jaringan LAN

5. Penulis dapat mengetahui hal-hal yang dapat meningkatkan keamanan pada jaringan LAN
6. Penulis dapat belajar menggunakan *software* HPING3 dan NMAP
7. Manfaat umum yaitu dapat digunakan sebagai acuan dalam penelitian berikutnya.